IN THE CLAIMS:

Please CANCEL claims 2, 9, 14 and 18 without prejudice.

Please AMEND claims 1, 3, 4, 5, 7, 10, 13, 15, 16, 19-21 and 23 as follows:

1. (Amended) A system for detecting and selectively removing viruses in data transfers, the system comprising:

a memory for storing data and routines, the memory having inputs and outputs, the memory including a server for scanning data for a virus and specifying data handling actions dependent on an existence of the virus;

a communications unit for receiving and sending data in response to control signals, the communications unit having an input and an output; [and]

a processing unit for receiving signals from the memory and the communications unit and for sending signals to the memory and communications unit; the processing unit having inputs and outputs; the inputs of the processing unit coupled to the outputs of memory and the output of the communications unit; the outputs of the processing unit coupled to the inputs of memory, the input of the communications unit, the processor controlling and processing data transmitted through the communications unit to detect viruses and selectively transfer data depending on the existence of viruses in the data being transmitted[.];

a proxy server for receiving data to be transferred, the proxy server scanning the data to be transferred for viruses and controlling transmission of the data to be transferred according to preset handing instructions and the presence of viruses, the proxy server having a data input, a data output

and a control output, the data input coupled to receive the data to be transferred; and

a daemon for transferring data from the proxy server in response to control signals from the proxy server, the daemon having a control input, a data input and a data output, the control input of the daemon coupled to the control output of the proxy server for receiving control signals, and the data input of the daemon coupled to the data output of the proxy server for receiving the data to be transferred.

Al cont.

Av

23. (Amended) The system of claim [2] 1, wherein the proxy server is a FTP proxy server that handles evaluation and transfer of data files, and the daemon is an FTP daemon that communicates with a recipient node and transfers data files to the recipient node.

24. (Amended) The system of claim [2] 1, wherein the proxy server is a SMTP proxy server that handles evaluation and transfer of messages, and the daemon is an SMTP daemon that communicates with a recipient node and transfers messages to the recipient node.

25. (Amended) A computer implemented method for detecting viruses in data transfers between a first computer and a second computer, the method comprising the steps of:

receiving at a server a data transfer request including a destination address;

B

electronically ~~transmitting~~ receiving data ~~to~~ at the server;

determining whether the data contains a virus at the server;

performing a preset action on the data using the server if the data contains a virus; [and]

sending the data to the destination address if the data does not contain a virus[.];

determining whether the data is of a type that is likely to contain a virus; and

transmitting the data from the server to the destination without performing the steps of determining whether the data contains a virus and performing a preset action, if the data is not of a type that is likely to contain a virus.

A3

~~7.~~ 6. (Amended) The method of claim ~~6~~ 5, wherein the step of scanning is performed using [in] a signature scanning process.

A4

~~10.~~ 8. (Amended) The method of claim [9] ~~8~~ 4, wherein the step of determining whether the data is of a type that is likely to contain a virus is performed by comparing an extension type of a file name for the data to a group of known extension types.

A5

~~13.~~ 11. (Amended) A computer implemented method for detecting viruses in a mail message transferred between a first computer and a second computer, the method comprising the steps of:

receiving a mail message request including a destination address;

B

electronically ~~transmitting~~ receiving the mail message ~~to~~ at a server;

determining whether the mail message contains a virus, the determination of whether the mail message contains a virus comprising determining whether the mail message includes any encoded portions, storing each encoded portion of the mail message in a separate temporary file, decoding the encoded portions of the mail message to produced decoded portions of the mail message, scanning each of the decoded portions for a virus, and testing whether the scanning step found any viruses;

A5 concl.

performing a preset action on the mail message if the mail message contains a virus; and

sending the mail message to the destination address if the mail message does not contains a virus.

---

12 11
~~15~~. (Amended) The method of claim [14] ~~12~~, wherein the step of [scanning] determining whether the mail message [for] includes any encoded portions searches for uuencoded portions.

A12

13
~~16~~. (Amended) [The method of claim 14, wherein:] A computer implemented method for detecting viruses in a mail message transferred between a first computer and a second computer, the method comprising the steps of:

receiving a mail message request including a destination address;

B electronically ~~transmitting~~ receiving the mail message ~~to~~ at a server;

scanning the mail message for encoded portions;

determining whether the mail message contains a virus;

performing a preset action on the mail message if the mail message contains a virus;

sending the mail message to the destination address if the mail message does not contains a virus; and

wherein the step of sending the mail message to the destination address is performed if the mail message does not contain any encoded portions; the server includes a SMTP proxy server and a SMTP daemon; and the step of sending the mail message comprises transferring the mail message from the SMTP proxy server to the SMTP daemon [,] and transferring the mail message from the SMTP daemon to a node having an address matching the destination address.

AP Cancl.

A.1

15 ~~19~~. (Amended) The method of claim [18] 11 ~~13~~, wherein step of scanning is performed using [in] a signature scanning process.

16 ~~20~~. (Amended) The method of claim [14] 11 ~~13~~, wherein the step of performing a preset action on the mail message comprises performing one step from the group of:

transferring the mail message unchanged;

not transferring the mail message;

storing the mail message as a file with a new name and notifying a recipient of the mail message request of the new file name; and

creating a modified mail message by writing the output of the determining step into the modified mail message and transferring the mail message to the destination address.

17 11
21. (Amended) The method of claim [18] ~~12~~, wherein the step of performing a preset action on the mail message comprises performing one step from the group of:

A1 Cont.

transferring the mail message unchanged;

transferring the mail message with the encoded portions having a virus deleted; and

renaming the encode portions of the mail message containing a virus, and storing the renamed portions as files in a specified directory on the server and notifying a recipient of the renamed files and directory; and

writing the output of the determining step into the mail message in place of respective encoded portions that contain a virus to create a modified mail message and sending the modified mail message.

A8

19 18
23. (Amended) The apparatus of claim ~~22~~, wherein means for determining includes a means for scanning that scans the data using [in] a signature scanning process.
